Federal Bureau of Investigation
Office of Public Affairs
National Press Office

Public Affairs Guidance

POC : AD Michael P. Kortan [redacted] b6 b7C
POC: UC [redacted]
PAS [redacted]

Topic: Going Dark, Encryption, and the National Domestic Communications Assistance Center

Press Guidance:

Talking Points and Q & A's below are ~~**for internal use only**~~. Use these to assist preparing SAC or others for any interviews or inquiries. Do not disseminate this paper in this format. Field Offices media reps should handle all local media queries. Calls referring to cases of a national significance can be referred to NPO UC [redacted] or PAS [redacted] b6 b7C

Background:

[redacted] b5 b7E

Q & As:

Has the Going Dark problem gotten worse for law enforcement over the past year? How?

The impediments faced by law enforcement have been getting worse for quite some time. As technology continues to advance, new services introduced, and the number of providers increase, law enforcement faces an increasing number of diverse challenges.

Many of the newest communications services are developed and deployed without consideration of law enforcement's lawful intercept needs. Under current law there is no requirement for many companies to do so. Communications Assistance to Law Enforcement Act (CALEA), last updated in 2005, applies only to traditional telecommunications carriers, providers of interconnected Voice over Internet Protocol (VoIP) services, and providers of broadband access services.

What is the FBI's reaction to the announcement from Apple that their phones will include encryption that the company is not able to unlock, even in response to a court order? How will this impact the FBI's investigative abilities?

Although the FBI is unable to discuss specific companies or technical investigative capabilities, the FBI continues to be extremely concerned about the serious threat posed by the increasing proliferation of encryption technology that prevents access to critical evidence obtained through lawful electronic surveillance. The FBI and our law enforcement partners remain committed to working with Congress and the telecommunications industry to ensure lawful access to critical evidence obtained through electronic surveillance and/or search and seizure.

What about workarounds? Can't law enforcement retrieve the same information through metadata, the Cloud, or through guessing the password on the phone?

Metadata, which includes telephone records, email logs, and location information obtained from phone carriers, does provide useful information to law enforcement. But that information is incomplete, difficult to access when time is of the essence, and does not provide the content of any communication.

The FBI may be able to access data via the Cloud with a search warrant, but that will not yield information stored on a device that is not backed up by the Cloud. Plus, many devices have a setting whereby data is erased after too many failed attempts to break a password.

Many criminal adversaries pay close attention to law enforcement's vulnerabilities and continually seek ways to exploit vulnerabilities. It is vital that law enforcement retain capabilities to access the types of information needed to protect and serve the American people.

Has the FBI experienced any reduced cooperation from communication providers as a result of the disclosures attributed to Edward Snowden?

Yes. A number of the country's largest providers have been openly vocal about their concerns regarding surveillance and have published an open letter to the President and members of Congress. Law enforcement has no issue with these companies' commitment to *"keeping users' data secure — deploying the latest encryption technology to prevent unauthorized surveillance on our networks and by pushing back on government requests to ensure that they are legal and reasonable in scope."*

What is missing is a vigorous commitment to assist law enforcement when electronic

surveillance is authorized. It is vitally important to distinguish between law enforcement's use of lawfully authorized electronic surveillance and "bulk collection."

What is needed is an open and frank dialogue about the responsibilities of industry to assist law enforcement. Industry and law enforcement need to move forward and develop a framework under which both sides participate in striking an appropriate balance among the public's privacy interests, the industry's goals of competition and innovation, and the needs of law enforcement.

Why does law enforcement believe companies should be forced to build in backdoors when designing services? Don't backdoors pose a security risk for companies?

That's a common misperception of what law enforcement needs and what law enforcement is requesting. Law enforcement is not asking for unfettered access into any provider's network. As part of the ideal CALEA process – the industry develops a technical standard through its normal specification processes; a provider controls the technical solution resident in its network; it ensures its network is capable of isolating only the target identified in the court order; it activates the interception; and it disables the interception when the order expires. Law enforcement is only the recipient of the information collected by the provider. This is a "front door" approach – where law enforcement first gains the lawful authority and then serves the provider with the court order that directs the provider to conduct the intercept.

It's important to stress that an open, transparent process for identifying technical capabilities benefits everyone. First, the public can be assured that the capabilities are commensurate with the already existing authorities granted to law enforcement by statute. Second, the industry understands its responsibilities and all providers are held to the same standard (i.e., a level playing field). Third, law enforcement can be confident that it will receive what it needs and is authorized by law to collect, regardless of the specific service provider.

Law enforcement believes that providers can minimize any risks by developing intercept solutions during the service's design phase. Such solutions are likely to be better, smarter, cheaper, and more secure than solutions that are retrofitted to existing products. There was similar apprehension during the initial stages of discussions about CALEA – that there would be an increased security risk in having technical solutions resident in carriers' networks. That prediction has not come to pass.

How many companies or applications does the FBI encounter where you know they will not provide real time data?

There are hundreds of communication service providers that offer new services which do not have an electronic surveillance capability. This number continues to grow as technology continues to evolve.

Wiretap law requires a company or individual to provide "technical assistance" to an official with a valid electronic surveillance order. Does the phrase "technical assistance" so vague that it leads to differences of interpretation?

Yes. The "technical assistance" clause in federal wiretap law is often insufficient. The assistance furnished by some providers simply does not provide law enforcement with the information it requested and which it needs to fully understand or acquire the relevant

communications. It is more than a difference of interpretation in that, without more specific guidance as to what constitutes "technical assistance," a provider may do all that it can and still not be able to provide law enforcement the information it needs to do its job.

As a practical matter, a CALEA compliant provider who has a built an intercept capability into its architecture will most likely be able to assist law enforcement immediately, whereas a provider that has no solution and attempts to render "technical assistance" likely will not. In most instances, providers attempting to render assistance must divert resources to react to an immediate situation, such as a hostage-taking or kidnapping scenario, where time is of the essence. Despite their best efforts, critical information will be lost due to the delay.

It has been reported the government receives a daily dump of screen shots from companies. Why is this not good enough?

In some cases subject to legal process, it may be enough that law enforcement receives a daily report of the lawfully authorized information. But in many instances, the information is incomplete or not provided in a timely manner to support every type of investigative requirement, especially when dealing with crimes in motion (e.g., kidnapping, extortion, drug trafficking). Also, not every company has the capability. Further, there is significant disparity in what companies offering similar services can provide to law enforcement – there is simply a lack of consistency across the board.

There is also an issue with law enforcement receiving "screen shots" in that they are typically no more than a picture file. Law enforcement needs the information in a format that is readily usable for effective analysis.

Law enforcement believes a mandate would necessitate a vitally important discussion about what providers must furnish to law enforcement in response to a court order. Importantly, that discussion would result in uniformity in the information law enforcement can expect from providers and what companies can expect to provide.

How does FBI respond when companies outright refuse to comply with a court order? How many times do you take that company to court?

The primary court-based recourse available to law enforcement is to pursue an order to show cause. In essence, a court would require a company to explain why it cannot meet the requirements of the court's order to assist in the implementation of an interception. The decision to pursue show cause orders is very case-specific and can in some instances spur a company to be more responsive. However, this process often extends well beyond the time limitations of the original court order and historically has not proven to be an effective use of already scarce law enforcement resources.

Is it true that that there has never been a fine issued under either CALEA or the 2518 provision of the Wiretap Act? Why not?

It is true that fines have not been issued under the CALEA enforcement provisions set forth in Title 18 U.S.C. Section 2522 which, in turn, incorporate the provisions of Section 108 of CALEA. As written, the enforcement provisions are cumbersome and the pursuit of enforcement can be a lengthy, complicated, and resource-intensive process. In many cases, the investigation which identified the capability gap would be closed long before any action would be taken.

However, it is not correct to imply that the enforcement provision of the law cannot have any effect. The enforcement provision allows law enforcement to raise non-compliance issues to the attention of a company's senior management and work toward a common understanding of the company's obligations. Law enforcement and prosecutors are more interested in ensuring companies have the appropriate capabilities at their disposal when served with a court order than pursuing fines or penalties through prolonged litigation of the underlying issues, but this option remains viable, if needed.

Does the FBI favor new electronic surveillance capability laws or see a need to update existing laws such as CALEA?

In certain respects, today's ever-widening gap between technology and law enforcement's electronic surveillance capabilities is not a new phenomenon. For decades, law enforcement has struggled to keep pace with evolving communications technology, periodically requiring congressional intervention to align law enforcement capabilities with new technological realities. The difference today is the sheer pace at which communications technology is advancing. Each passing year brings a dramatic increase in the volume of communications, the sophistication and complexity of communications service offerings, and the number of communications service providers. The same technology fueling this rapid innovation, however, is simultaneously making lawful interception of modern communications services increasingly less feasible for law enforcement. Unless corrective action is taken, law enforcement's electronic surveillance capabilities will continue to erode and potentially become obsolete.

How will passage of the Domestic Retention and Investigatory Powers (DRIP) legislation in the United Kingdom, which requires companies to retain customer communications data, impact the Going Dark problem in the US?

It is premature to comment on how the UK legislation will impact United States law enforcement's ability to effect court orders. However, it does reflect the fact that the UK is facing a similarly daunting challenge in conducting electronic surveillance.

NDCAC

The FBI has launched the NDCAC. Is it working as expected? Can I learn more about the NDCAC?

Yes. The NDCAC was designed as a hub for technical knowledge management that facilitates the sharing of solutions and know-how among law enforcement agencies, and strengthens law enforcement's relationships with the communications industry. The NDCAC leverages / shares law enforcement's collective technical knowledge and resources on issues involving real-time and stored communications to address challenges posed by advanced communications services and technologies. But, it can't solve all of law enforcement's problems – it allows a certain measure of self-help within the community. The entire community still necessarily relies on industry's assistance.

It is important to note that the NDCAC does not conduct research and development, is not responsible for the execution of any electronic surveillance court orders, and does not have any direct operational or investigative role in investigations. Rather, the NDCAC provides technical knowledge and referrals in response to requests for assistance from any member

of the law enforcement community. The NDCAC also leverages the training capabilities of certain law enforcement agencies to benefit a larger portion of the community.

More information is available on the website: http://www.ndcac.cjis.gov

What is the NDCAC?

The National Domestic Communications Assistance Center (NDCAC) is designed as a hub for technical knowledge management that facilitates the sharing of solutions and know-how among law enforcement agencies. The NDCAC leverages and shares collective technical knowledge and resources of federal, state, and local law enforcement with respect to electronic surveillance capabilities, evidence collection on communications devices, and technical location capabilities, as well as works to strengthen law enforcement's relationships with the communications industry. The NDCAC operates a 24/7 held desk for immediate assistance, and maintains a staff of subject matter experts to provide technical knowledge and referrals in response to requests from any member of the law enforcement community.

It is important to point out that NDCAC does not conduct research and development, is not responsible for the actual execution of any electronic surveillance court orders, and does not have any direct operational role in investigations. Rather, it provides technical knowledge and referrals in response to law enforcement's requests for technical assistance.

Where is the NDCAC located and how is it staffed?

The NDCAC is a Department of Justice organized facility operated by the FBI on behalf of the law enforcement community. It is located in Fredericksburg, Virginia, and is staffed with technical experts dedicated to supporting the entire law enforcement community. Its staff is comprised of agents from the four DOJ law enforcement component agencies: Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATFE), Drug Enforcement Administration (DEA), FBI, and United States Marshals Service (USMS). In addition, the NDCAC has engineers and support personnel on staff.

How long has the NDCAC been operational and why are we only learning about this now?

Congress initially funded NDCAC in fiscal year 2012, and since that time the Center has worked to locate and outfit the facility, hire a large portion of its staff, and implement rules and policies. The NDCAC has been able to provide limited assistance to the law enforcement community during this stand-up phase and will provide more comprehensive support to the law enforcement community as it reaches full functionality.

Will the NDCAC train state and local law enforcement how to eavesdrop on internet-based and mobile communications?

The NDCAC offers a wide variety of training to the law enforcement community. The primary focus of the NDCAC's training is to raise law enforcement's level of understanding of new and emerging communications services and technologies and its impact on electronic surveillance capabilities, evidence collection on communications devices, and technical location capabilities.The NDCAC leverages existing training made available by the FBI and

other federal, state, and local law enforcement agencies. It also develops its own courses to fill in any gaps.

Technical personnel from other federal, state, and local law enforcement agencies are able to obtain advice and guidance if they have difficulty implementing lawful electronic surveillance court orders.

Does this increase in law enforcement's ability to monitor communications of innocent Americans pose a threat to civil liberties?

First, the NDCAC is not responsible for the actual execution of any electronic surveillance court orders and does not have any direct operational role in investigations.

Second, with respect to law enforcement investigations, it is important to emphasize that we are only talking about lawful, court-ordered intercepts in ongoing investigations. When investigators cannot collect communications pursuant to court order in near real-time, they may be unable to act quickly to disrupt threats or to protect public safety. In order to intercept electronic communications, law enforcement must have a court-order authorizing the intercept.

Furthermore, FBI employees carry out their mission according to an established set of rules and with full respect for the constitutional and statutory rights of the people. The FBI's Domestic Investigations and Operations Guide (DIOG) establishes the FBI's internal rules and procedures to implement the *Attorney General's Guidelines for Domestic FBI Operations* (AGG-Dom). The DIOG and AGG-Dom were promulgated in late 2008 to ensure that the FBI is equipped with all lawful and appropriate tools so that it can transform itself into an intelligence-driven organization that assesses and investigates criminal and national security threats to our nation and its people.

The NDCAC has been described as a secretive Internet-surveillance unit tasked with inventing technology to eavesdrop on web-based and mobile communications. Is this true?

No. There is nothing secret about the NDCAC. It is housed in a publicly identified location with a public website (http://www.ndcac.cjis.gov) and a publicly available budget. Additionally, NDCAC received guidance from an executive advisory board whose meetings are open to the public.

The NDCAC does not conduct research and development, is not responsible for the actual execution of any electronic surveillance court orders, and does not have any direct operational role in investigations.

Additionally, the FBI does not randomly intercept electronic communications. FBI investigative activity follows an established set of rules with full respect for the constitutional and statutory rights of the people. In order to intercept electronic communications the FBI must have a predicated investigation and a court-order authorizing the intercept.

Is it true that the NDCAC is working with specific communications providers to develop "back-doors" to facilitate law enforcement surveillance of user accounts?

No. The NDCAC does work with industry in a number of different ways. Specifically, the NDCAC identifies law enforcement's electronic surveillance needs, works to understand providers' capabilities, and validates that those industry solutions work. Neither the NDCAC nor law enforcement requests or has the ability to control providers' solutions. Rather, each provider is responsible for its respective solution and provides to law enforcement any intercepted communications only with the appropriate lawful authorization.

Is the NDCAC charged with creating customized surveillance technologies aimed at a specific individual or company?

No. The NDCAC does not conduct research and development into electronic surveillance solutions. Further, the NDCAC is not responsible for the actual execution of any electronic surveillance court orders, and does not have any direct operational role in investigations. Rather, the NDCAC provides technical knowledge and referrals in response to law enforcement's requests for technical assistance. Those referrals allow law enforcement to leverage existing solutions, to the extent they exist, that may not be otherwise readily available.